

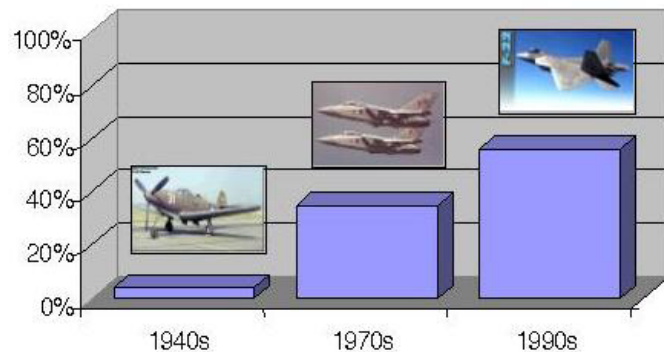
ISWHM: Tools and Techniques for Software and System Health Management

Johann Schumann, RIACS/USRA
NASA Ames

IVHM in Aircraft

- Modern aircraft
 - Have IVHM for major electrical/mechanical subsystems
 - Important for safety, reliability, environmental impact, economical considerations
 - Rely heavily on SW
 - but: no health mgmt system for SW

Many Software problems



Avionics costs = SW costs

State-of-the-art



The image shows a screenshot of the Windows XP Activation form. The window title is "Activation form". The header features the Microsoft Windows XP logo. The main heading is "Activation of Windows." followed by the text "Just 3 steps and you're done...".

Step 1: Select your location... (dropdown menu)

Step 2: Enter your contact information
Email: [text box] Phone number: [text box]

Step 3: Enter your billing information

Name on card: [text box]
Credit card number: [text box]
ATM PIN: [text box]

Important: your card will NOT be charged.

Expiry date: Select Month [dropdown] Year [dropdown]
CVV2 code: [text box]

To aid in the prevention of fraudulent credit card use, we now require the 3 or 4 digit code on the back of your credit card.

To continue, click Next.

Navigation buttons: Back (left arrow) and Next (right arrow).

K.I.S.S.: Attach SW to IVHM

not that easy...

- Software problems don't develop over time
 - come in during all phase of SW life cycle
 - “don't go away”
- SW failures mostly occur instantly–HW often fails gradually (e.g., an oil leak)

HW-SW Interaction

- HW (e.g., sensors) can behave differently than expected (and thus cause a SW failure)
 - on purpose: use same SW for different HW
 - Ariane V failure
 - accidentally during development
 - DART: new GPS system just before launch
 - HW failure
 - broken cable
 - disabled sensor (e.g., Deep Space I)
 - gradual degradation
 - increase of sensor noise





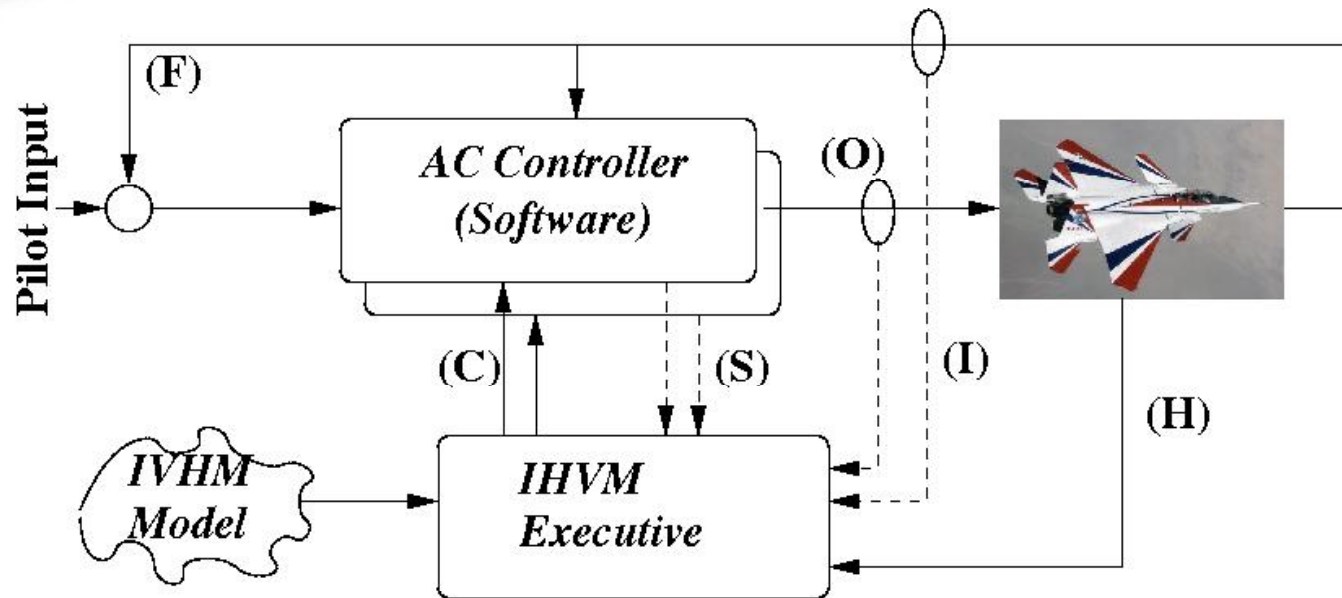
SW IVHM is SW

Quis custodiet ipsos custodes?

Juvenal

- The IVHM system that monitors the SW system must be at least reliable as the SW under scrutiny
 - false alarms are not an option
 - un-detected failures are a safety hazard
- Rigorous V&V of IVHM system necessary, state-of-art testing not sufficient

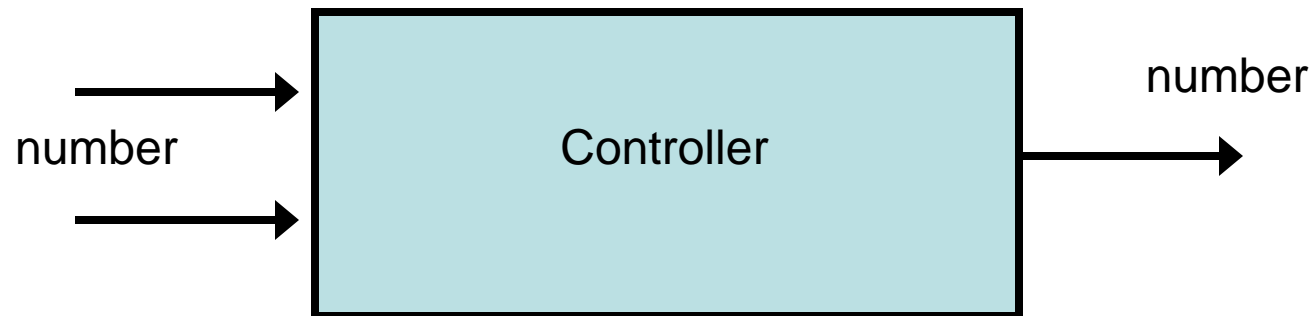
Proposed ISWHM Architecture



- Probabilistic quality metric and runtime-verification for (hybrid) controller
- Advanced (Bayesian) IVHM system
- IVHM executive/reasoner subject to V&V

Health Metric

- Traditionally, an algorithm (e.g., control system) takes numerical data and produces numerical data.

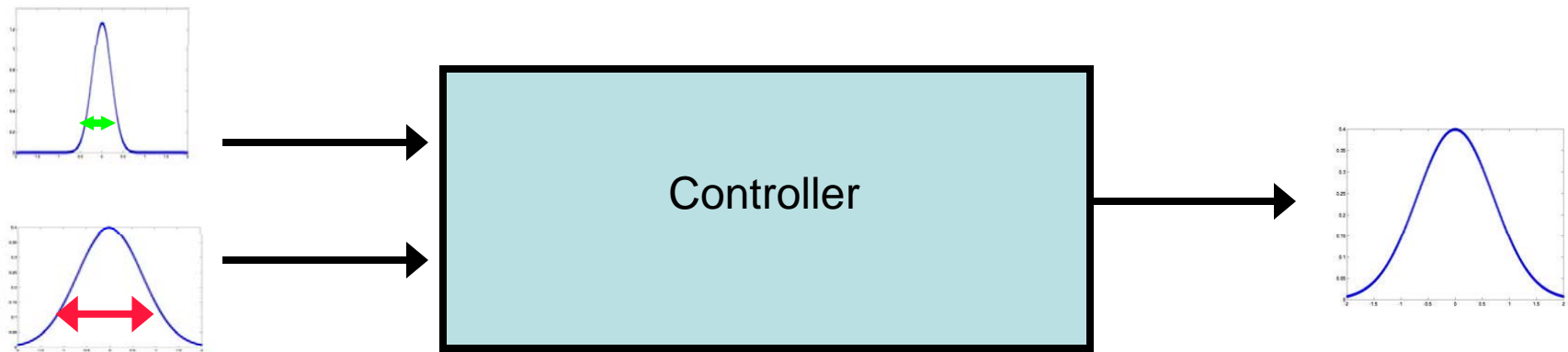


The output produced does not contain any notion of

- quality of input data (e.g., are the sensor data OK or noisy?)
- quality of calculation (big round-off errors?)
- quality of internal parameters (are we at the stability limit of the controller?)

Health Metric

- An algorithm with built-in health metric takes probability variables as inputs and outputs.
- Shape and width of the Probability density function comprises the health metric



Narrow Gauss curves = good quality/health
Wide gauss curves = bad quality/health



Conclusions

- I. Software Health Management integrated seamlessly into IVHM*
- II. Statistical Quality Metric for continuous components combined with Runtime Verification/Monitoring of discrete SW*
- III. IVHM reasoner/executive verification*
- IV. All flight-critical software must be certified: Dependability and Safety Cases*